JOHN M. NEUKOM (SBN 275887)
JAMES Y. PAK (SBN 304563)
SKADDEN, ARPS,
SLATE, MEAGHER & FLOM LLP
525 University Avenue
Palo Alto, California 94301-1908
Telephone: (650) 470-4500
Facsimile: (650) 470-4570
john.neukom@skadden.com
james.pak@skadden.com

DOUGLAS R. NEMEC (*pro hac vice* – to be filed)
RACHEL R. BLITZER (*pro hac vice* – to be filed)
LESLIE A. DEMERS (*pro hac vice* – to be filed)
SKADDEN, ARPS,
SLATE, MEAGHER & FLOM LLP
One Manhattan West
New York, New York 10001
Telephone: (212) 735-3000
Facsimile: (212) 735-2000
douglas.nemec@skadden.com
rachel.blitzer@skadden.com
leslie.demers@skadden.com

Attorneys for Plaintiff,
Fortinet, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

FORTINET, INC., Plaintiffs, vs. FORESCOUT TECHNOLOGIES, INC., Defendant.	Case No. **COMPLAINT FOR PATENT INFRINGEMENT** JURY TRIAL DEMANDED

Plaintiff Fortinet, Inc. (Fortinet) demands a trial by jury on all issues so triable and brings this action for patent infringement against Defendant Forescout Technologies, Inc. (Forescout) as follows:

NATURE OF THE ACTION

1. This is a civil action for patent infringement under the patent laws of the United States, 35 U.S.C. § 1, *et seq.*

2. This action seeks legal and equitable relief against Forescout's unlawful infringement of Fortinet's United States Patent Nos. 8,458,314 (the '314 patent), 9,369,299 (the '299 patent), and 9,948,662 (the '662 patent) (together, the Asserted Patents) generally relating to cybersecurity technology.

3. Fortinet is a market-leading innovator of cybersecurity products, software, and services. Fortinet's research and development, innovation, and patents represent an enormous investment of time and capital in cybersecurity innovation over the past twenty years. Forescout has wrongfully incorporated Fortinet's intellectual property into its product offerings, and Forescout and its customers are infringing in a material way that goes to the heart of Forescout's business.

PRELIMINARY STATEMENT

4. Fortinet was founded in 2000 with a mission to innovate and develop substantive, multi-faceted cybersecurity technology to help protect its customers, which include some of the world's largest healthcare providers, educational institutions, and critical infrastructure and telecommunications providers. Over the last two decades, Fortinet has invested substantially in research and development in order to provide the best protection possible for its customers. Since bad actors attack organizations through different threat vectors, Fortinet's approach has been to develop a "security fabric" of broad defensive security innovations to protect its customers from hackers trying to breach their organizations.

5. As part of Fortinet's mission in providing cybersecurity protections, in 2018 it acquired Bradford Networks, Inc. (Bradford), a leading innovator in network access control (NAC) security technology. Bradford was founded in 2002 and was an early pioneer in certain security solutions, including NAC technology, and security for the Internet of Things (IoT) and guest management. Among other innovations, Bradford invented the first Adaptive Network Security (ANS) platform solution to dynamically adapt to changing security needs by automatically responding and securely provisioning network resources based on pre-established policies. Bradford's solutions uniquely identify and profile devices and users to provide visibility and control. Bradford's commercial solutions include its Network Sentry family of security products, which feature built-in network security and policy management software in a hardware appliance (or set of appliances), visibility into and control of users and devices on a campus network to prevent unauthorized access and to keep the network secure, and management technology to ensure secure network access for guest users and to simplify the administration of guest accounts.

6. While Fortinet and Bradford have remained steadfast in their commitment to cybersecurity innovations, Defendant Forescout's business focus by contrast has changed over the years. Forescout currently, like Fortinet, sells security technology to businesses. But rather than innovate on its own, Forescout instead has followed Fortinet's and Bradford's technological leadership. For example, long after Bradford introduced its Network Sentry and ANS platforms, Forescout followed suit, releasing its CounterACT platform. Further, long after Bradford began developing NAC technology, Forescout pivoted its business model and started to do the same.

7. The different strategic paths taken by Fortinet and Forescout have been reflected in the market. Fortinet is now the top grossing cybersecurity company in many regions. Fortinet recently announced its quarterly revenue increased 22% over the prior year, and it is generating a profit, a testament to its innovation value-add to its customers. Relatedly, Fortinet's stock was one

of the best performing stocks of the last decade, and the market currently values Fortinet at approximately $23 billion. With steady leadership since its founding—guided by its founders, both engineers who have focused on security their entire careers—Fortinet has grown to over 7,000 employees and over 400,000 customers. Fortinet's focus on, and investment in, innovation and development of industry-leading security products has led to both world-class security offerings and a world-class patent portfolio, with over 600 issued U.S. patents and 149 additional patent applications pending before the U.S. Patent and Trademark Office (USPTO).

8. Forescout, on the other hand, has floundered as it has tried to follow the lead of companies like Fortinet and others, and Forescout's results and the market's reaction reflect this. Forescout has lost hundreds of millions of dollars and recently reported a material drop in its sales, a 24% year over year decrease, to $57 million this past quarter, with a greater loss, a loss of $60 million. Forescout's stock has struggled, and its current market valuation is about 6% of Fortinet's. And Forescout recently entered an agreement to be acquired by a private equity firm, firms that often cut spending by, and investment in, floundering acquired companies in areas such as research and development and customer support, thereby further stifling innovation and customer satisfaction, in an effort to improve the companies' profitability and cashflow.

9. In order to meet its responsibilities, Fortinet is committed to protecting and the defending intellectual property that it and Bradford worked so diligently to develop. Fortinet does not take litigation lightly; throughout its history, Fortinet has engaged in lawsuits to protect its intellectual property only on seldom occasions. Fortinet prefers to avoid litigation and instead to work in good faith with infringers to address any infringement.

10. Accordingly, on February 27, 2020, Fortinet attempted to initiate licensing discussions with Forescout, with the good faith objective to engage in reasonable business discussions in order to reach an amicable business agreement to resolve Forescout's infringement.

Fortinet offered patent- and business-related information to Forescout designed to help Forescout analyze Fortinet's position and respond, including background regarding Fortinet and its patent portfolio and a detailed licensing proposal, and requested further discussions so that Fortinet could provide additional information.

11. Thereafter, Fortinet continued make substantial attempts to engage with Forescout, including correspondence on March 11, March 17, March 23, March 24, March 27, April 10, April 13, April 21, April 22, April 29, April 30, and May 7. Despite Fortinet's repeated efforts to address the infringement amicably and in good faith, Forescout has delayed progressing the discussions for almost three months. Throughout its communications with Forescout, Fortinet repeatedly requested the opportunity to meet or speak with Forescout, offering to respond to any questions and provide additional detail on the call. Forescout, however, refused to have any conversation with Fortinet for over two months, repeatedly evading any discussion, and to-date Forescout has refused to have its internal business employees discuss this matter with business representatives of Fortinet. And it was only after many requests by Fortinet and months of delay and evasion by Forescout that Forescout ultimately gave Fortinet the opportunity to have a phone call, not with any business representatives of Forescout, but with Forescout's outside counsel, which did not occur until April 24, 2020.

12. On the April 24 call, Fortinet provided Forescout with additional substantive information, including the identification of specific patents that are infringed by Forescout's technology, and detail regarding Fortinet's prior licensing practices. Fortinet responded to Forescout's questions during that call. In response to Fortinet sharing information and asking questions, Forescout committed to respond the next week but then reneged on that commitment. As of the filing of this Complaint, Forescout still has not indicated a willingness to remedy its unauthorized use of Fortinet's intellectual property, or given an indication that they are in fact engaging in good faith discussions to try to do so.

13. Fortinet is filing this lawsuit to protect its intellectual property and to stop the material infringement by Forescout.

THE PARTIES

14. Fortinet is a Delaware corporation with a principal place of business at 899 Kifer Road, Sunnyvale, California 94086.

15. Upon information and belief, Forescout is a Delaware corporation with a principal place of business at 190 West Tasman Drive, San Jose, California 95134.

JURISDICTION AND VENUE

16. This is a civil action for patent infringement pursuant to 35 U.S.C. § 271.

17. This Court has subject matter jurisdiction over the matters asserted herein under 28 U.S.C. §§ 1331 and 1338(a), and 35 U.S.C. § 281, because this is a matter arising under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq*.

18. Forescout is subject to this Court's personal jurisdiction because it resides, maintains its headquarters, and does business in the state of California. In addition, upon information and belief, Forescout has committed substantial acts of infringement giving rise to this action and regularly conducts business within this judicial District, including by maintaining its headquarters in this District. For example, Forescout has purposefully and voluntarily placed one or more of its infringing products, as described below, into the stream of commerce with the expectation that these infringing products will be used in this District. On information and belief, these infringing products have been and continue to be used in this District.

19. This Court therefore has personal jurisdiction over Forescout.

20. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391 and 1400(b) because Forescout is subject to personal jurisdiction in this District; resides in this District; maintains its

headquarters in this District; regularly conducts business in this District; and committed and continues to commit acts of patent infringement in this District.

FACTUAL BACKGROUND

Fortinet's History of Innovation

21. Founded in 2000 by serial entrepreneurs and technology visionaries Ken and Michael Xie, Fortinet is one of the world's leading providers and innovators of network security technologies, including deep security protection technology, with tens of thousands of customers worldwide including enterprises, carriers, data centers, distributed offices, and governments. Fortinet currently employs over 7,000 employees around the world—including thousands of engineers—and has shipped over five million units to over 400,000 customers globally. Fortinet's inventions form the core of modern network, fabric, and cloud security technology and enable secure business communications around the world.

22. Over the past 20 years, Fortinet has invested substantial resources researching and developing its technologies related to its cybersecurity products and services through the expenditure of considerable employee work hours and company resources. Fortinet's research and development has led to numerous innovative products in the network security market as well as valuable intellectual property. Fortinet's industry-leading research and development efforts—together with selective acquisitions—have resulted in a portfolio of over 600 patents issued in the United States, with another 149 U.S. patent applications pending.

23. Since its founding, one of Fortinet's core focuses has been designing, developing, and improving network security systems to protect businesses from cyber-attacks. Fortinet's FortiGate appliances, for example, target content-based cyber threats from email and web traffic. By integrating a broad suite of deep security protection technology, Fortinet helps protect its customers with its comprehensive security solutions. Fortinet has won dozens of awards for its network security

innovations,[1] and more recently in 2019 Fortinet was recognized as being a "Magic Quadrant" Leader for Network Firewalls.[2]

24. Bradford Networks developed a policy-based security automation and orchestration platform that enables discovery of endpoint and network infrastructure devices, including, but not limited to the FortiGate, FortiSwitch, FortiAP, and FortiWLC. Bradford Network's solutions provide contextual awareness for implementing dynamic network access control, and provide the ability to contain a cyber breach through automated threat response. By automating the complex threat triage process and rapidly responding to security alerts from security solutions like FortiGate, FortiSIEM and FortiAnalyzer, Bradford Network's Network Sentry reduces the risk of unauthorized access to corporate assets and intellectual property, and reduces the impact, time, and costs of containing cyber threats.

25. The proliferation of IoT devices has made it necessary for organizations to improve their visibility into what is attached to their networks. They need to know every device and every user accessing their networks. While IoT devices enable digital transformation initiatives and improve efficiency, flexibility, and optimization, they are inherently untrustworthy, with designs that prioritize low-cost over security. Accordingly, the IoT revolution has raised a new challenge for network owners. How can one see and protect against a myriad of devices showing up on the network?

26. Network Access Control has come back to the forefront of security solutions to address that challenge. Fortinet has a solution for these problems, FortiNAC. FortiNAC provides network visibility to see devices connected to a network as well as the ability to control those devices and users, including dynamic, automated responses.

---

[1] *E.g.*, *Fortinet Industry Awards*, https://www.fortinet.com/corporate/about-us/industry-awards.html.

[2] *Fortinet Recognized as a Leader in the Gartner Magic Quadrant for Network Firewalls*, Fortinet (Sep. 18, 2019), https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2019/leader-10th-time-gartner-mq-network-firewalls.html.

27. This technology that was originally developed to assist with bring-your-own-device (BYOD) policies, and ensure devices met the endpoint compliance policies of the institutions allowing BYOD, is now getting renewed focus as a means to safely accommodate headless IoT devices in the network. FortiNAC enables three key capabilities to secure IoT devices:

- Network visibility to see every device and user as they attempt to join the network;
- Network control to limit where devices can go on the network; and
- Automated response to speed the reaction time to events from days to seconds.

28. Collectively, these capabilities provide tools that network owners need to secure a world that is embracing IoT. The FortiNAC solution protects wireless, wired, and VPN networks with a centralized architecture that enables distributed deployments with automated responsiveness.

29. As large organizations continue to see high growth in network traffic and the number of devices and users accessing their networks, the risk of breach increases exponentially. According to a recent Forrester study, 82 percent of companies surveyed are unable to even identify all devices accessing their networks. The integration of Bradford Networks' technology with Fortinet's security fabric enables large enterprises with visibility, micro-segmentation and access control technology to help contain threats and block untrusted devices from accessing the network

THE ASSERTED PATENTS

30. The '314 patent, issued on June 4, 2013, is titled "System and method for offloading IT network tasks." Frank D. Andrus, Paula Jane Dunigan, Todd R. Wohlers, Paul D. Playdon, and Alan R. Hackert are the named inventors. Fortinet is the current owner by assignment of the '314 patent. A true and correct copy of the '314 patent is attached hereto as Exhibit A.

31. The '299 patent, issued on June 14, 2016, is titled "Network access control system and method for devices connecting to network using remote access control methods." Eric P. Dupont, Seshakrishnan Srinivasan, and Frank D. Andrus are the named inventors. Fortinet is the current

owner by assignment of the '299 patent. A true and correct copy of the '299 patent is attached hereto as Exhibit B.

32. The '662 patent, issued on April 17, 2018, is titled "Providing security in a communication network." Robert A. May is the named inventor. Fortinet is the current owner by assignment of the '662 patent. A true and correct copy of the '662 patent is attached hereto as Exhibit C.

ACTS GIVING RISE TO THIS ACTION

33. The allegations provided below are exemplary and without prejudice to Fortinet's infringement contentions. In providing these allegations, Fortinet does not convey or imply any particular claim constructions or the precise scope of the claims. Fortinet's claim construction contentions regarding the meaning and scope of the claim terms will be provided under the Court's scheduling order and local rules.

34. On information and belief, the infringing Forescout products include, but are not limited to, ForeScout CounterACT, Forescout CounterACT Appliance (CT-R, CT-100, CT-1000, CT-2000, CT-4000 and CT-10000), Forescout CounterACT Virtual Appliance (VCT-R, VCT-100, VCT-1000, VCT-2000, VCT-4000, VCT-10000), Forescout 5100 Series (5110, 5120, 5140 and 5160), Forescout SecureConnector, and Forescout Network Module, and related products and services identified below for each Asserted Patent in Counts I-III (Accused Products).

35. As detailed further below, each element of at least one claim of each of the Asserted Patents is literally present in the Accused Products, or is literally practiced by the method performed using the Accused Products. To the extent that any element is not literally present or practiced, each such element is present or practiced under the doctrine of equivalents.

COUNT I: INFRINGEMENT OF U.S. PATENT NO. 8,458,314

36. Fortinet incorporates by reference and re-alleges all the foregoing paragraphs of this Complaint as if fully set forth herein.

37. On information and belief, Forescout has induced or contributed to the infringement of at least claim 1 of the '314 patent by making, using, selling, offering for sale, and/or importing into the United States, without authority or license, for example, ForeScout CounterACT, Forescout CounterACT Appliance (CT-R, CT-100, CT-1000, CT-2000, CT-4000 and CT-10000), Forescout CounterACT Virtual Appliance (VCT-R, VCT-100, VCT-1000, VCT-2000, VCT-4000, VCT-10000), Forescout 5100 Series (5110, 5120, 5140 and 5160), Forescout SecureConnector, and Forescout Network Module (collectively, the '314 Accused Products). The '314 Accused Products are non-limiting examples that were identified based on publicly available information, and Fortinet reserves the right to identify additional infringing activities, products and services, including, for example, on the basis of information obtained during discovery.

38. Forescout has induced and continues to induce infringement of at least claim 1 of the '314 Patent under 35 U.S.C. § 271(b).

39. Forescout indirectly infringes the '314 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform some of the steps of the method claims, either literally or under the doctrine of equivalents, of the '314 Patent, where all the steps of the method claims are performed by either Forescout or its customers, purchasers, users and developers, or some combination thereof. Forescout knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users and developers, to infringe by practicing, either themselves or in conjunction with Forescout, one or more method claims of the '314 Patent, including claim 1 through use of, for example, ForeScout CounterACT.

40. Forescout knowingly and actively aided and abetted the direct infringement of the '314 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '314 Accused Products. Such instructions and encouragement included, but are not limited to, advising third parties to use the '314 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '314 Patent, and by advertising and promoting the use of the '314 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '314 Accused Products in an infringing manner. For example, Forescout maintains a Resources website with support, technical documentation, training, and blogs with information about operating Forescout's products (available at https://www.forescout.com/company/resources/).

41. By at least the filing of this Complaint, Fortinet disclosed the existence of the '314 patent and identified at least some of Forescout's and others' activities that infringe the '314 patent. Thus, based on this disclosure, Forescout had knowledge of the '314 patent, including claim 1, and that its activities infringe the '314 patent, including claim 1, since at least the filing of the Complaint. Based on Fortinet's disclosures, Forescout has also known or should have known since at least the filing of the Complaint that its customers, distributors, suppliers, and other purchasers of the '314 Accused Products are infringing the '314 patent, including claim 1.

42. On information and belief, Forescout further contributes to the infringement of one or more claims of the '314 patent under 35 U.S.C. § 271(c) by offering to sell, selling, and/or importing into the United States a component of the '314 Accused Products, or a material or apparatus for use in practicing a process claimed in the '314 patent, that constitutes a material part of the inventions, knowing the same to be especially made or especially adapted for use in an infringement of the '314 patent, including claim 1, and is not a staple article or commodity of commerce suitable for substantial noninfringing use.

43. The '314 Accused Products meet all the limitations of at least claim 1 of the '314 patent. Specifically, claim 1 of the '314 patent recites: a method for control of computer network resources connected to a computer network supporting network endpoints by delegating control from a network administrator to at least one sponsor comprising the steps of: creating templates for users and devices of said computer network by said network administrator at an administrator account on a workstation connected to said computer network; creating profiles used to control said resources of said computer network; associating said templates with said profiles; creating at least one said sponsor by said network administrator; associating, by said network administrator, at least one of said profiles with said sponsor; delegating, by said network administrator, network management administrative privileges to said sponsor, transferring responsibility for said users and devices from said network administrator to said sponsor when said template of said users and devices is associated with said profile of said sponsor; and controlling of said computer network resources by said sponsor, using said templates assigned to said sponsor by said network administrator, wherein said sponsor is constrained by said network administrator by said at least one associated profile, said sponsors not having network management administrative privileges over said network administrator.

44. The use of the '314 Accused Products constitutes practicing the claimed invention of the '314 Patent because their use amounts to a method of delegating control of computer network access from network administrators to sponsors. The network administrator creates templates and profiles that associate network users with a sponsor and controlling use of network resources. Using the '314 Accused Products, a network administrator delegates network management administrative privileges to a sponsor, and transfers responsibility for particular users to the sponsor. For example, the Forescout 5100 Series products are Network Access Control products, creating templates, profiles for devices and users and creating sponsors for guest users.

45. This description is based on publicly available information and a reasonable investigation of the structure and operation of the '314 Accused Products. Exemplary materials that describe infringement through the use of '314 Accused Products can be found on Forescout's website: https://www.forescout.com/wp-content/uploads/2018/11/counteract-administration-guide-8.0.1.pdf, https://www.forescout.com/company/resources/guest-management-operators-how-to-guide-8-0/.

46. As a result of Forescout's unlawful activities, Fortinet has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law, especially given that Fortinet and Forescout both compete in the security software space.

47. Forescout's continued infringement of the '314 Patent causes harm to Fortinet in the form of price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages are insufficient to compensate Fortinet for these harms. Accordingly, Fortinet is entitled to injunctive relief.

48. Forescout's infringement of the '314 Patent has furthermore injured and continues to injure Fortinet in an amount to be proven at trial, but not less than a reasonable royalty and/or the lost profits that Fortinet would have made but-for Forescout's acts of infringement.

49. Despite its knowledge of Fortinet's patent portfolio and Asserted Patents, Forescout continues to sell the Accused Products and services in complete and reckless disregard of Fortinet's patent rights. As such, Forescout is acting recklessly and continues to willfully, wantonly, and deliberately engage in acts of infringement of the '314 Patent, making this an exceptional case and justifying an award to Fortinet of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT II: INFRINGEMENT OF U.S. PATENT NO. 9,369,299

50. Fortinet incorporates by reference and re-alleges all the foregoing paragraphs of this Complaint as if fully set forth herein.

51. On information and belief, Forescout has induced or contributed to the infringement of at least claim 1 of the '299 patent by making, using, selling, offering for sale, and/or importing into the United States, without authority or license, for example, ForeScout CounterACT, Forescout CounterACT Appliance (CT-R, CT-100, CT-1000, CT-2000, CT-4000 and CT-10000), Forescout CounterACT® Virtual Appliance (VCT-R, VCT-100, VCT-1000, VCT-2000, VCT-4000, VCT-10000), Forescout 5100 Series (5110, 5120, 5140 and 5160), Forescout SecureConnector, and Forescout Network Module (collectively, the '299 Accused Products). The '299 Accused Products are non-limiting examples that were identified based on publicly available information, and Fortinet reserves the right to identify additional infringing activities, products and services, including, for example, on the basis of information obtained during discovery.

52. Forescout has induced and continues to induce infringement of at least claim 1 of the '299 Patent under 35 U.S.C. § 271(b).

53. Forescout indirectly infringes the '299 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to use the system of the claims, either literally or under the doctrine of equivalents, of the '299 Patent, where all components of the system of the claims are provided by either Forescout or its customers, purchasers, users and developers, or some combination thereof. Forescout knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users and developers, to infringe by using, either themselves or in conjunction with Forescout, they system of one or more claims of the '299 Patent, including claim 1, through use of, for example, ForeScout CounterACT.

54. Forescout knowingly and actively aided and abetted the direct infringement of the '299 Patent, including claim 1, by instructing and encouraging its customers, purchasers, users and developers to use the '299 Accused Products. Such instructions and encouragement included, but are not limited to, advising third parties to use the '299 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '299 Patent, and by advertising and promoting the use of the '299 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '299 Accused Products in an infringing manner. For example, Forescout maintains a Resources website with support, technical documentation, training, and blogs with information about operating Forescout's products (available at https://www.forescout.com/company/resources/).

55. By at least the filing of this Complaint, Fortinet disclosed the existence of the '299 patent and identified at least some of Forescout's and others' activities that infringe the '299 patent, including claim 1. Thus, based on this disclosure, Forescout had knowledge of the '299 patent and that its activities infringe the '299 patent, including claim 1, since at least the filing of the Complaint. Based on Fortinet's disclosures, Forescout has also known or should have known since at least the filing of the Complaint that its customers, distributors, suppliers, and other purchasers of the '299 Accused Products are infringing the '299 patent, including claim 1.

56. On information and belief, Forescout further contributes to the infringement of one or more claims of the '299 patent, including claim 1, under 35 U.S.C. § 271(c) by offering to sell, selling, and/or importing into the United States a component of the '299 Accused Products, or a material or apparatus for use in practicing a process claimed in the '299 patent, that constitutes a material part of the inventions, knowing the same to be especially made or especially adapted for use in an infringement of the '299 patent, including claim 1, and is not a staple article or commodity of commerce suitable for substantial non-infringing use.

57. The '299 Accused Products meet all the limitations of at least claim 1 of the '299 patent. Specifically, claim 1 of the '299 patent recites: A system for out-of-band control of network access supporting multiple connections comprising: a network comprising a server device, at least one terminal device, and a communication link between them; at least one remote access device (RAD) comprising memory, and communicatively coupled to said network; and a Network Access Control Server (NACS) comprising memory, controlling said network access, wherein said network access control is out of band and comprises: identity management of said connections; endpoint compliance of said connections; and usage policy enforcement of said connections; wherein said enforcement is out of band and is accomplished on said RAD, comprising communicating with said RAD to make real-time changes to its running configuration, whereby said enforcement is vendor-independent and said system is RAD-agnostic; said network access control comprising receiving a connect attempt to said network from a user device; said RAD authenticating connecting user to said NACS for said out of band network control; said NACS capturing RAD identification, location; restricting access to said network by said user device with a network access filter (NAF) configured on said RAD; said RAD directing said client device to an agent; on said user device, running said agent; said agent identifying client to said NACS; modifying said NAF based on compliance; and monitoring post-connection of successful connections.

58. The use of the '299 Accused Products constitutes practicing the claimed invention of the '299 Patent, including claim 1, because their use amounts to a system of for out-of-band control of network access as claimed. The '299 Accused Products as used include a network with a server device and terminal device, communicatively linked, and at least one remote access device (RAD). For example, the '299 Accused Products include a VPN Concentrator plugin that allows remote devices to connect to a network. The '299 Accused Products as used also include a Network Access Control Server (NACS) that controls network access and includes identity management of

connections, endpoint compliance of connections, and usage policy enforcement of connections, with the enforcement accomplished on the RAD with real-time changes to its running configuration. For example, the use of the '299 Accused Products includes the use of a VPN Concentrator Plugin to also track users, disconnect them from the VPN, and prevent them from reconnecting. This enforcement is vendor-independent and this system is RAD-agnostic, with the '299 Accused Products supporting server packages such as Cisco VPN 3000, Cisco VPN ASA 5500 Series Adaptive Security Appliance, Juniper 5.5R1, and Nortel V07_00.062. A connect attempt from user device is received, the RAD authenticates the connecting user to the NACS, and the NACS captures RAD identification, location. For example, the use of the '299 Accused Products includes capturing of VPN-related information such as VPN IP. The use of the '299 Accused Products restricts access to the network by the user device with a network access filter (NAF) configured on the RAD. The RAD directs the client device to an agent, the agent is run on the user device, and the agent identifies the client to the NACS. For example, the use of the '299 Accused Products includes the use of SecureConnector running from a client device, with the SecureConnector sending a unique ID to help identify the endpoint. NAF is modified based on compliance, and successful connections are monitored post-connection.

59. This description is based on publicly available information and a reasonable investigation of the structure and operation of the '299 Accused Products. Exemplary materials that describe infringement through the use of '299 Accused Products can be found on Forescout's website: https://www.forescout.com/wp-content/uploads/2018/11/counteract-administration-guide-8.0.1.pdf, https://www.forescout.com/company/resources/vpn-concentrator-plugin-configuration-guide-4-1/, https://www.forescout.com/company/resources/hps-inspection-engine-configuration-guide-11-0/, https://www.forescout.com/company/resources/counteract-deploying-secure-connector-service-part-machine-image-guide/.

60. As a result of Forescout's unlawful activities, Fortinet has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law, especially given that Fortinet and Forescout both compete in the security software space.

61. Forescout's continued infringement of the '299 Patent causes harm to Fortinet in the form of price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages are insufficient to compensate Fortinet for these harms. Accordingly, Fortinet is entitled to injunctive relief.

62. Forescout's infringement of the '299 Patent has furthermore injured and continues to injure Fortinet in an amount to be proven at trial, but not less than a reasonable royalty and/or the lost profits that Fortinet would have made but-for Forescout's acts of infringement.

63. Despite its knowledge of Fortinet's patent portfolio and Asserted Patents, Forescout continues to sell the Accused Products and services in complete and reckless disregard of Fortinet's patent rights. As such, Forescout has acted recklessly and continues to willfully, wantonly, and deliberately engage in acts of infringement of the '299 Patent, making this an exceptional case and justifying an award to Fortinet of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT III: INFRINGEMENT OF U.S. PATENT NO. 9,948,662

64. Fortinet incorporates by reference and re-alleges all the foregoing paragraphs of this Complaint as if fully set forth herein.

65. On information and belief, Forescout has induced or contributed to the infringement of at least claim 1 of the '662 patent by making, using, selling, offering for sale, and/or importing into the United States, without authority or license, for example, ForeScout CounterACT, Forescout CounterACT Appliance (CT-R, CT-100, CT-1000, CT-2000, CT-4000 and CT-10000), Forescout

CounterACT Virtual Appliance (VCT-R, VCT-100, VCT-1000, VCT-2000, VCT-4000, VCT-10000), Forescout 5100 Series (5110, 5120, 5140 and 5160), Forescout SecureConnector, and Forescout Network Module (collectively, the '662 Accused Products). The '662 Accused Products are non-limiting examples that were identified based on publicly available information, and Fortinet reserves the right to identify additional infringing activities, products and services, including, for example, on the basis of information obtained during discovery.

66. Forescout has induced and continues to induce infringement of at least claim 1 of the '662 Patent under 35 U.S.C. § 271(b).

67. Forescout indirectly infringes the '662 Patent, including claim 1, pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform some of the steps of the method claims, either literally or under the doctrine of equivalents, of the '662 Patent, where all the steps of the method claims are performed by either Forescout or its customers, purchasers, users and developers, or some combination thereof. Forescout knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users and developers, to infringe by practicing, either themselves or in conjunction with Forescout, one or more method claims of the '662 Patent, including claim 1, through use of, for example, ForeScout CounterACT.

68. Forescout knowingly and actively aided and abetted the direct infringement of the '662 Patent, including claim 1, by instructing and encouraging its customers, purchasers, users and developers to use the '662 Accused Products. Such instructions and encouragement included, but are not limited to, advising third parties to use the '662 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '662 Patent, including claim 1, and by advertising and promoting the use of the '662 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '662 Accused Products in

an infringing manner. For example, Forescout maintains a Resources website with support, technical documentation, training, and blogs with information about operating Forescout's products (available at https://www.forescout.com/company/resources/).

69. By at least the filing of this Complaint, Fortinet disclosed the existence of the '662 patent and identified at least some of Forescout's and others' activities that infringe the '662 patent, including claim 1. Thus, based on this disclosure, Forescout had knowledge of the '662 patent and that its activities infringe the '662 patent, including claim 1, since at least the filing of the Complaint. Based on Fortinet's disclosures, Forescout has also known or should have known since at least the filing of the Complaint that its customers, distributors, suppliers, and other purchasers of the '662 Accused Products are infringing the '662 patent, including claim 1.

70. On information and belief, Forescout further contributes to the infringement of one or more claims of the '662 patent, including claim 1, under 35 U.S.C. § 271(c) by offering to sell, selling, and/or importing into the United States a component of the '662 Accused Products, or a material or apparatus for use in practicing a process claimed in the '662 patent, that constitutes a material part of the inventions, knowing the same to be especially made or especially adapted for use in an infringement of the '662 patent, including claim 1, and is not a staple article or commodity of commerce suitable for substantial noninfringing use.

71. The '662 Accused Products meet all the limitations of at least claim 1 of the '662 patent. Specifically, claim 1 of the '662 patent recites: A method comprising: receiving, by a network security device within an enterprise network, an application protocol request directed to an external network that is originated by a client device associated with the enterprise network; determining, by the network security device, based on the application protocol request whether a network parameter of the external network is associated with a set of trusted networks; and selectively disabling, by the network security device, application of a subset of security features of a plurality of security features

to be applied to network traffic exchanged between the client device and the external network while the client device is accessing the external network when a result of said determining is affirmative, wherein the subset of security features are selected based on a trust level associated with the external network.

72. The use of the '662 Accused Products constitutes practicing the claimed invention of the '662 Patent because their use amounts to a method of providing security in a communication network as claimed, including in claim 1. The '662 Accused Products provide a network security device that receives an application protocol request directed to an external network, originated by a client device associated with the network. A network security device determines whether a network parameter of the external network is associated with a set of trusted networks based on that application protocol request. For example, the '662 Accused Products define Legitimate Traffic based on source information such as source or destination address. Further, when this determining is affirmative, a network security device selectively disables application of security features based on a trust level associated with the external network, to be applied to network traffic exchanged between the client device and the external network while the client device is accessing the external network. For example, the '662 Accused Products disables features such as Threat Protection features based on traffic type.

73. This description is based on publicly available information and a reasonable investigation of the structure and operation of the '662 Accused Products. Exemplary materials that describe infringement through the use of '662 Accused Products can be found on Forescout's website: https://www.forescout.com/wp-content/uploads/2018/11/counteract-administration-guide-8.0.1.pdf, https://www.forescout.com/company/resources/packet-engine-configuration-guide-8-1/.

74. As a result of Forescout's unlawful activities, Fortinet has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law, especially given that Fortinet and Forescout both compete in the security software space.

75. Forescout's continued infringement of the '662 Patent causes harm to Fortinet in the form of price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages are insufficient to compensate Fortinet for these harms. Accordingly, Fortinet is entitled to injunctive relief.

76. Forescout's infringement of the '662 Patent has furthermore injured and continues to injure Fortinet in an amount to be proven at trial, but not less than a reasonable royalty and/or the lost profits that Fortinet would have made but-for Forescout's acts of infringement.

77. Despite its knowledge of Fortinet's patent portfolio and Asserted Patents, Forescout continues to sell the Accused Products and services in complete and reckless disregard of Fortinet's patent rights. As such, Forescout has acted recklessly and continues to willfully, wantonly, and deliberately engage in acts of infringement of the '662 Patent, making this an exceptional case and justifying an award to Fortinet of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

PRAYER FOR RELIEF

WHEREFORE, Fortinet respectfully requests:

1. That Judgment be entered that Forescout has infringed one or more of the Asserted Patents, literally or under the doctrine of equivalents;

2. That, in accordance with 35 U.S.C. § 283, Forescout and all affiliates, employees, agents, officers, directors, attorneys, successors, and assigns and all those acting on behalf of or in active concert or participation with any of them, be permanently enjoined from (1) infringing the

Asserted Patents and (2) making, using, selling, offering for sale and/or importing the Accused Products;

3. An award of damages sufficient to compensate Fortinet for Forescout's infringement under 35 U.S.C. § 284, beginning no later than the filing of this Complaint;

4. That the case be found exceptional under 35 U.S.C. § 285 and that Fortinet be awarded its attorneys' fees;

5. Costs and expenses in this action;

6. An award of prejudgment and post-judgment interest; and

7. Such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Fortinet respectfully demands a trial by jury on all issues so-triable, raised by this Complaint.

DATED: May 15, 2020

Respectfully submitted,

SKADDEN, ARPS,
SLATE, MEAGHER & FLOM, LLP

By: /s/ John M. Neukom
John M. Neukom

JOHN M. NEUKOM (SBN 275887)
JAMES Y. PAK (SBN 304563)
SKADDEN, ARPS,
SLATE, MEAGHER & FLOM LLP
525 University Avenue
Palo Alto, California 94301-1908
Telephone: (650) 470-4500
Facsimile: (650) 470-4570
john.neukom@skadden.com
james.pak@skadden.com

DOUGLAS R. NEMEC (pro hac vice – to be filed)
RACHEL R. BLITZER (pro hac vice – to be filed)
LESLIE A. DEMERS (pro hac vice – to be filed)
SKADDEN, ARPS,
SLATE, MEAGHER & FLOM LLP
One Manhattan West
New York, New York 10001
Telephone: (212) 735-3000
Facsimile: (212) 735-2000
douglas.nemec@skadden.com
rachel.blitzer@skadden.com
leslie.demers@skadden.com

Attorneys for Plaintiff,
Fortinet, Inc.